EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	"6820202".pn.	USPAT	OR	OFF	2006/11/06 07:53
L2	3837	wheeler.inv.	US-PGPUB; USPAT	OR	OFF	2006/11/06 07:54
L3	4	2 and lynn and ann	US-PGPUB; USPAT	OR	OFF	2006/11/06 07:54
L4	57	2 and greenwood	US-PGPUB; USPAT	OR	OFF	2006/11/06 08:35
L5	7385	380/255 or 713/176 or 713/181 or 713/156 or 713/175 or 713/182 or 705/57 or 705/64	US-PGPUB; USPAT	OR	OFF	2006/11/06 08:37
L6	99	5 and encod$3 and compar$3 and "public key" and "private key" and authenticat$3 and message and account and sender and information and communication and identity and predetermin$2 and function	US-PGPUB; USPAT	OR	OFF	2006/11/06 08:40
L7	84	6 and validat$3 and associat$3	US-PGPUB; USPAT	OR	OFF	2006/11/06 08:40
L8	80	7 and identity and retriev$4	US-PGPUB; USPAT	OR	OFF	2006/11/06 08:40
L9	571	encod$3 and compar$3 and "public key" and "private key" and authenticat$3 and message and account and sender and information and communication and identity and predetermin$2 and function and associat$3 and identity and validat$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/11/06 08:42
L10	84	5 and 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/11/06 08:42

NPL Search Please Scan

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

encod$3 and compar$3 and "public key" and "private key" and

THE ACM DIGITAL LIBRARY

Terms used **encod$3** and **compar$3** and **public key** and **private key** and **authenticat$3** and **message** and **account** and **sender** and **information** and **communication** and **identi**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Results 1 - 20 of 200

Best 200 shown

Result page: **1** 2 3 4 5 6 7 8 9 10

1 New basic technologies for DIM: Pseudonym management using mediated identity-based
Thibault Candebat, Cameron Ross Dunne, David T. Gray
November 2005 **Proceedings of the 2005 workshop on Digital identity management DIM**
Publisher: ACM Press
Full text available: pdf(293.16 KB) Additional Information: full citation, abstract,

Mobile Location-Based Services (LBS) have raised privacy concerns amongst mobile phone use
untrustworthy third parties in order to access these applications. Widespread acceptance of suc
handled in order to restore users' confidence in what could become the "killer app" of 3G netwo

Keywords: SEM architecture, identity-based encryption, location-based services, pseudonymit

2 Privacy/anonymity: Receiver anonymity via incomparable public keys
Brent R. Waters, Edward W. Felten, Amit Sahai
October 2003 **Proceedings of the 10th ACM conference on Computer and communicat**
Publisher: ACM Press
Full text available: pdf(230.49 KB) Additional Information: full citation, abstract,

We describe a new method for protecting the anonymity of message receivers in an untrusted r
anonymity for receivers (although those methods do protect sender anonymity). Our method re
we call an Incomparable Public Key cryptosystem, which allows a receiver to efficiently create r

Keywords: PGP, anonymity, privacy, public key cryptography

3 Trust, recommendations, evidence, and other collaboration know-how (TRECK): Strong ps
Michael Kinateder, Ralf Terdic, Kurt Rothermel
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '0.**
Publisher: ACM Press
Full text available: pdf(231.59 KB) Additional Information: full citation, abstract,

In this paper we present a novel approach to enable untraceable communication between pseu
eliminating the need to know of each other's address.We use a variation of Chaum mixes to ac
called *extended destination routing* (EDR) which relies on routing headers constructed in multip

Keywords: data protection, distributed reputation systems, extended destination routing, mixe

4 Role-based access control on the web
Joon S. Park, Ravi Sandhu, Gail-Joon Ahn
February 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume
Publisher: ACM Press
Full text available: pdf(331.03 KB) Additional Information: full citation, abstract,

Current approaches to access control on the Web servers do not scale to enterprise-wide syster were motivated by the need to manage and enforce the strong and efficient RBAC access contr we identify two different architectures for RBAC on the Web, called user-pull and server-pull. Tc

Keywords: WWW security, cookies, digital certificates, role-based access control

5 Secure communications between bandwidth brokers
Bu-Sung Lee, Wing-Keong Woo, Chai-Kiat Yeo, Teck-Meng Lim, Bee-Hwa Lim, Yuxiong He, Jie Son
January 2004 **ACM SIGOPS Operating Systems Review**, Volume 38 Issue 1
Publisher: ACM Press
Full text available: pdf(922.33 KB) Additional Information: full citation, abstract,

In the Differentiated Services (DiffServ) architecture, each domain has a Bandwidth Broker to p multi-domain environment, Simple Inter-domain Bandwidth Broker Signaling (SIBBS) protocol bandwidth broker communication. Since the information exchanged between BBs are sensitive inter-domai ...

Keywords: Bandwidth Broker, Public Key Infrastructure, Simple Inter-domain Bandwidth Brok

6 Authentication in distributed systems: theory and practice
Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4
Publisher: ACM Press
Full text available: pdf(3.37 MB) Additional Information: full citation, abstract,

We describe a theory of authentication and a system that implements it. Our theory is based or simple principal either has a name or is a communication channel; a compound principal can ex reason about a principal's authority by deducing the other principals that it can speak for; auth

Keywords: certification authority, delegation, group, interprocess communication, key distribu for, trusted computing base

7 Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world
Marjory S. Blumenthal, David D. Clark
August 2001 **ACM Transactions on Internet Technology (TOIT)**, Volume 1 Issue 1
Publisher: ACM Press
Full text available: pdf(176.33 KB) Additional Information: full citation, abstract,

This article looks at the Internet and the changing set of requirements for the Internet as it bec wider set of purposes. We discuss a set of principles that have guided the design of the Interne the range of new requirements now emerging could have the consequence of compromising the

Keywords: ISP, Internet, end-to-end argument

8 Just fast keying: Key agreement in a hostile internet
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis,
May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume
Publisher: ACM Press
Full text available: pdf(324.39 KB) Additional Information: full citation, abstract,

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use ir
proof of the latter property. JFK also has a number of novel engineering parameters that permi
perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: Cryptography, denial-of-service attacks

9 Atomicity in electronic commerce
J. D. Tygar
May 1996 **Proceedings of the fifteenth annual ACM symposium on Principles of distribut**
Publisher: ACM Press
Full text available: pdf(1.74 MB) Additional Information: full citation, references, citings, index terms

10 Integrating security in inter-domain routing protocols
Brijesh Kumar, Jon Crowcroft
October 1993 **ACM SIGCOMM Computer Communication Review**, Volume 23 Issue 5
Publisher: ACM Press
Full text available: pdf(1.35 MB) Additional Information: full citation, abstract,

Network routing protocols work in a vulnerable environment. Unless protected by appropriate s
capable of modifying, deleting or adding false information in routing updates. This paper first ai
then proposes various counter measures to make these protocols secure against external threa

11 Content-triggered trust negotiation
Adam Hess, Jason Holt, Jared Jacobson, Kent E. Seamons
August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume
Publisher: ACM Press
Full text available: pdf(815.36 KB) Additional Information: full citation, abstract,

The focus of access control in client/server environments is on protecting sensitive server resou
resources. The set of resources is usually static, and an access control policy associated with ea
article, we turn the traditional client/server access control model on its head and address how t

Keywords: Trust negotiation, access control, authentication, credentials

12 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for int
William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelo
November 2002 **Proceedings of the 9th ACM conference on Computer and communicati**
Publisher: ACM Press
Full text available: pdf(118.52 KB) Additional Information: full citation, abstract,

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Ar
property. JFK also has a number of novel engineering parameters that permit a variety of trade
secrecy against susceptibility to denial-of-service attacks.

Keywords: cryptography, denial of service attacks

13 Security enhanced mobile agents
Vijay Varadharajan
November 2000 **Proceedings of the 7th ACM conference on Computer and communications**
Publisher: ACM Press
Full text available: pdf(393.46 KB) Additional Information: full citation, references, citings, inc

Keywords: mobile agents, secure agent based application, security model

14 Securing the global, remote, mobile user
Walt Curtis, Lori Sinton
March 1999 **International Journal of Network Management**, Volume 9 Issue 1
Publisher: John Wiley & Sons, Inc.
Full text available: pdf(982.14 KB) Additional Information: full citation, abstract,

Electronic commerce is inevitable and will reshape our lives, but before true electronic commerc
enterprise against outside attacks on its electronic information and provide controls for authoriz

15 Encryption and Secure Computer Networks
Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, inc

16 Data integrity: The HP time vault service: exploiting IBE for timed release of confidential in
Marco Casassa Mont, Keith Harrison, Martin Sadler
May 2003 **Proceedings of the 12th international conference on World Wide Web**
Publisher: ACM Press
Full text available: pdf(860.87 KB) Additional Information: full citation, abstract,

Digital information is increasingly more and more important to enable interactions and transact
can have harmful effects for people, enterprises and governments.This paper focuses on the pr
simplifying its access once public: it is a common issue in the industry, government and day-to

Keywords: disclosure policies, identifier-based encryption, privacy, security, timed-release, we

17 SPV: secure path vector routing for securing BGP
Yih-Chun Hu, Adrian Perrig, Marvin Sirbu
August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the :**
protocols for computer communications SIGCOMM '04, Volume 34 Issue 4
Publisher: ACM Press
Full text available: pdf(236.82 KB) Additional Information: full citation, abstract,

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of t
Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. S
deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of m
se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

18 Johnny 2: a user test of key continuity management with S/MIME and Outlook Express
Simson L. Garfinkel, Robert C. Miller
July 2005 **Proceedings of the 2005 symposium on Usable privacy and security SO**
Publisher: ACM Press
Full text available: pdf(665.63 KB) Additional Information: full citation, abstract,

Secure email has struggled with signifcant obstacles to adoption, among them the low usability
certificates. Key continuity management (KCM) has been proposed as a way to lower these bar
signing essentially automatic. We present the first user study of KCM-secured email, conducted

Keywords: Usability, e-commerce, user interaction design, user studies

19 Ad hoc networks: The security of vehicular ad hoc networks
Maxim Raya, Jean-Pierre Hubaux
November 2005 **Proceedings of the 3rd ACM workshop on Security of ad hoc and sensoı**
Publisher: ACM Press
Full text available: pdf(283.96 KB) Additional Information: full citation, abstract,

Vehicular networks are likely to become the most relevant form of mobile ad hoc networks. In t
threat analysis and devise an appropriate security architecture. We also describe some major d
technical implications. We provide a set of security protocols, we show that they protect privacy

Keywords: security, vehicular ad hoc networks

20 Link and channel measurement: A simple mechanism for capturing and replaying wireless
Glenn Judd, Peter Steenkiste
August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental appı**
Publisher: ACM Press
Full text available: pdf(6.06 MB) Additional Information: full citation, abstract,

Physical layer wireless network emulation has the potential to be a powerful experimental tool.
accurately model the wireless channel. In this paper we examine the possibility of using on-carı
advantage of this approach is the simplicity and ubiquity with which these measurements can b

Keywords: channel capture, emulation, wireless

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 .